UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,982	08/16/2004	Makoto Izawa	27592-01102-US1	4981

30678 7590 03/11/2010
CONNOLLY BOVE LODGE & HUTZ LLP
1875 EYE STREET, N.W.
SUITE 1100
WASHINGTON, DC 20006

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	**PAPER NUMBER**
2437	
MAIL DATE	**DELIVERY MODE**
03/11/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/710,982	**Applicant(s)** IZAWA ET AL.	
	Examiner NADIA KHOSHNOODI	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 January 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to pending claims 1-19 (17-19 being newly added) filed 11/4/2009 have been fully considered but are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Response to Arguments

Applicants contend that Haney fails to teach that "portions of Haney specifically describe specifically describe how the disclosed firewall adds or strips IP addresses" and that "this affects routing and corresponds to an implementation of at least a portion of the network layer within the firewall." Examiner would like to note that stripping a packet header of an encapsulated packet does not indicate that a routing process has occurred. Specifically, Applicants claims call for "without any routing process at a network layer being performed," however there is no indication in the cited portion of Haney that the packet is "routed" from the LAN to the destination address since no path must be chosen from various possible routes. Since Haney teaches the packet is in close proximity with the destination address, stripping the packet header to obtain the destination address is merely used for forwarding the packet within the LAN as opposed to determining a path that it must take to travel via the WAN as occurs in a routing operation (par. 40, lines 14-24). Thus, Haney's stripping of the IP address does not affect routing and does not incorporate use of the network layer.

Applicants also contend that "neither the cited section of Balabine, nor any other section of Balabine discusses that the bridge of Balabine is implemented in the data link layer."

Examiner would like to point out that although Balabine does not specifically mention that the bridge implementing a firewall is on the data link layer, it was both publicly and commonly known at the time the invention was made that a bridge firewall is implemented on the data link layer (layer 2). Examiner would like to note that two different NPL documents supporting the notion of what a bridge firewall was defined as at the time the invention was made have been cited in the Notice of References Cited and a copy is attached. Therefore, since the cited portion of Balabine teaches/suggests that by configuring a firewall on a bridge access to a LAN is made more restrictive in col. 3, lines 49-54, Balabine teaches/suggests the limitation in question.

Applicants further contend Ellington fails to teach/suggest "data transmission processes are carried out in layers lower than the network layer." Examiner respectfully disagrees. Ellington et al. specifically discloses an embodiment which suggests the benefits of utilizing the data link layer, as opposed to the network layer, in an environment employing IPSEC (col. 7, lines 30-41). Ellington et al. also propose the added benefit that would be gained in utilizing the invention disclosed. Specifically, Ellington et al. suggest using an IP-Sec bridge and shifting the routing processing (i.e. data transmission) from the network layer to a lower layer, such as the data link layer, significantly enhances system performance in col. 7, lines 41-45. Thus, Ellington et al. teach/suggest a bridge means is an IP-Sec bridge means and data transmission processes are carried out in layers lower than the network layer.

Finally, Applicants contend that the newly added claims are "in contrast with, for example Haney, in which an IP address is changed during processing." Examiner respectfully disagrees. Haney teaches stripping the header of the encapsulated packet (par. 40) which is not equivalent to changing the network address of the destination associated with the data. The destination address associated with the data is just hidden while the packet is routed across the WAN (par. 40, lines 1-14). Then, once this packet is received at the trusted side, the packet header is removed so that the destination address is no longer hidden (par. 40, lines 14-23). Therefore, the destination address associated with the data is never changed, just hidden en route and Haney teaches processing the data received without changing a network address of a destination associated with the data.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-8 and 12-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haney, US Pub. No. 2006/0101262, and further in view of Balabine, US Patent No. 6,631,417.

As per claim 1:

Haney substantially teaches an encryption apparatus, comprising: a plurality of ports to at least one of which a terminal or network having an encrypting capability can be directly or indirectly connected (par. 38); encryption/decryption means for performing an encrypting process to apply encryption-based security and a decrypting process to remove encryption-based security on data being communicated between the terminal or network having the encrypting capability and another network or terminal coupled to one of the plurality of ports (par. 38); and a means for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, to be outputted as it is from another port without any routing process at a network layer being performed, the means being disposed within the apparatus along with the encryption/decryption means (par. 40, lines 14-23 and par. 49).

Not explicitly disclosed is a wherein the means is a bridge means and is in a data link layer. However, Balabine teaches a bridge (in a data link layer) that implements a firewall (col. 3, lines 45-56). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Haney to have a bridge means in the data link layer for performing the encrypting or decrypting. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Balabine suggests that by configuring a firewall on a bridge access to a LAN is made more restrictive in col. 3, lines 49-54.

As per claim 2:

Haney and Balabine substantially teach the apparatus according to claim 1. Furthermore, Haney teaches wherein the encryption/decryption means is adapted to perform the encrypting process and the decrypting process on data, so that the apparatus receives and retransmits data in the form of encrypted data from and to the terminal or network having the encrypting capability, and the encryption apparatus receives and retransmits the data in the form of non-encrypted data from and to a network or apparatus coupled to another port of the apparatus and having no encrypting capability (par. 40 and 49).

As per claim 3:

Haney and Balabine substantially teach an apparatus, comprising: a plurality of ports to at least one of which a terminal or network can be directly or indirectly connected (par. 38); encryption/decryption means for performing an encrypting process or a decrypting process on data which has been received with one of the plurality of ports and then has passed through a physical layer and a data link layer, the encrypting process or decrypting process generating encrypted data or decrypted data (par. 38); and means for passing the encrypted data or decrypted data to the data link layer and the physical layer without passing said data to a network layer in which routing between networks is controlled, and then sending said data to another port so as to be outputted from said port to another terminal or network coupled to the other port, the means disposed within the apparatus, along with the encryption/decryption means (par. 40, lines 14-23 and par. 49).

Not explicitly disclosed is a wherein the means is a bridge means and is in a data link layer. However, Balabine teaches a bridge (in a data link layer) that implements a firewall (col. 3, lines 45-56). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Haney to have a bridge means in the data link layer for performing the encrypting or decrypting. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Balabine suggests that by configuring a firewall on a bridge access to a LAN is made more restrictive in col. 3, lines 49-54.

As per claims 4 and 14:

Haney and Balabine substantially teach the apparatus/method according to claims 3 and 5. Haney teaches the apparatus further comprising setting information storage means for storing setting information for controlling the encrypting process and the decrypting process, wherein the encryption/decryption means controls the encrypting process and the decrypting process by comparing the setting information stored in the setting information storage means with header information of a data packet data received with one of the plurality of ports (par. 39).

As per claim 5:

Haney substantially teaches a method for performing an encrypting process and a decrypting process using an encryption/decryption apparatus, the apparatus comprising: performing the encrypting or decrypting process on data which has been received with a first one of a plurality of ports of the encryption/decryption apparatus from a first network or terminal coupled to the first one of the plurality of ports and then has passed through a data link layer and a physical layer of the encryption/decryption apparatus, to thereby obtain encrypted data or decrypted data (par. 38); and outputting the encrypted data or decrypted data from a second one of the plurality of the ports of the encryption/decryption apparatus through the physical layer and means of the encryption/decryption apparatus to a second network or terminal coupled to the second one of the plurality of ports, without passing said data to a network layer in which routing is controlled (par. 40, lines 14-23 and par. 49).

Not explicitly disclosed is a wherein the means is a bridge means and is in a data link layer. However, Balabine teaches a bridge (in a data link layer) that implements a firewall (col.

3, lines 45-56). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Haney to have a bridge means in the data link layer for performing the encrypting or decrypting. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Balabine suggests that by configuring a firewall on a bridge access to a LAN is made more restrictive in col. 3, lines 49-54.

As per claim 6:

Haney and Balabine substantially teach a system, comprising: the apparatus according to claim 1. Furthermore, Haney teaches a terminal or network having an encrypting capability which can be connected to the apparatus (par. 38).

As per claim 7:

Haney and Balabine substantially teach the system, comprising: a terminal or network having an encrypting capability; a terminal or network having no encrypting capability; and an apparatus according to claim 2. Furthermore, Haney teaches the system which can be connected between the terminal or network having the encrypting capability and the terminal or network having no encrypting capability (par. 38).

As per claim 8:

Haney and Balabine substantially teach the apparatus according to claim 2. Furthermore, Haney teach wherein the encryption/decryption means is configured to perform the decrypting process on encrypted data and then sends said data to a terminal or network having no encrypting capability when the apparatus receives said encrypted data from another terminal or network having an encrypting capability and retransmits said data to the terminal or network having no encrypting capability, and is configured to perform the encrypting process on non-encrypted data and then send said data to a terminal or network having an encrypting capability when the apparatus receives said non-encrypted data from another terminal or network having no encrypting capability and retransmits said data to the terminal or network having the encrypting capability (par. 39-40).

As per claim 12:

Haney and Balabine substantially teach the method according to claim 5. Furthermore, Haney teaches wherein said performing the encrypting or decrypting process comprises: performing the encrypting process and the decrypting process on data so that data is received from or transmitted to a terminal or network having encryption capability in the form of encrypted data and so that data is received from or transmitted to a terminal or network without encryption capability in the form of the non-encrypted data (par. 40 and 49).

As per claim 13:

Haney and Balabine substantially teach the method according to claim 12. Furthermore, Haney teaches wherein said performing the encrypting process and the decrypting process comprises: performing the decrypting process on encrypted data received from a terminal or network having encryption capability and destined for a terminal or network not having encryption capability; performing the encrypting process on data received from a terminal or network not having encryption capability and destined for a terminal or network having encryption capability (par. 39-40).

As per claim 15:

Haney and Balabine substantially teach the method according to claim 5. Furthermore, Haney teach wherein said outputting comprises outputting the encrypted data if the second terminal or network has encryption capability and outputting the decrypted data if the second terminal or network does not have encryption capability (par. 39-40).

As per claim 16:

Haney and Balabine substantially teach the apparatus according to claim 3. Furthermore, Haney teaches wherein the other network or terminal coupled to the other port has encryption capability in the case in which the encrypted data is passed and does not have encryption capability in the case in which the decrypted data is passed (par. 40 and 49).

As per claims 17 and 18:

Haney and Balabine substantially teach the apparatus according to claims 1 and 3. Furthermore, Haney teaches processing the data received without changing a network address of a destination associated with the data (par. 40).

As per claim 19:

Haney and Balabine substantially teach the method according to claim 5. Furthermore, Haney teaches wherein the data received with the first one of the plurality of ports is output, following the performing of the encrypting or decrypting process, without changing a network address of a destination associated with the data (par. 40).

III. Claims 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haney, US Pub. No. 2006/0101262, and Balabine, US Patent No. 6,631,417 as applied to claims 1, 3, and 5 above, and further in view of Ellington et al., US Patent No. 6,708,218.

As per claims 9-11:

Haney and Balabine substantially teach the apparatus/method of claims 1, 3, and 5. Furthermore, Balabine teaches data transmission processes are carried out in layers lower than the network layer (col. 3, lines 45-56). Not explicitly disclosed is wherein the bridge means is an IP-Sec bridge. However, Ellington et al. teach the use of IP-Sec packet filtering which utilizes functionality in the data link layer to determine what type of processing is required for the received frame and shifts what is normally processed on the network layer onto the data link layer (col. 7, lines 31-45). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Haney and Balabine for the bridge means to be an IP-Sec bridge and for the routing processing to be shifted from the network layer (layer 3) to the data link layer (layer 2). This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ellington et al. suggest using an IP-Sec bridge and shifting the routing processing from the network layer to a lower layer, such as the data link layer, significantly enhances system performance in col. 7, lines 41-45.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,640,248
2. US Patent No. 6,490,273
3. US Pub. No. 2003/0106067
4. US Pub. No. 2003/0014650

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
3/8/2010

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437